UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/754,378	01/09/2004	Bindu Rama Rao	200701924-2	7763

22879 7590 12/24/2009

HEWLETT-PACKARD COMPANY
Intellectual Property Administration
3404 E. Harmony Road
Mail Stop 35
FORT COLLINS, CO 80528

EXAMINER	
AGWUMEZIE, CHARLES C	

ART UNIT	PAPER NUMBER
3685	

NOTIFICATION DATE	DELIVERY MODE
12/24/2009	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

JERRY.SHORMA@HP.COM
ipa.mail@hp.com
laura.m.clark@hp.com

Office Action Summary	Application No.	Applicant(s)	
	10/754,378	RAO ET AL.	
	Examiner	Art Unit	
	CHARLES C. AGWUMEZIE	3685	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *13 October 2009*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,2 and 4-40* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-2 and 4-40* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *05/10/04*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on October 13, 2009 has been entered.

Acknowledgments

2. Applicant's amendment filed on October 13, 2009 is acknowledged. Accordingly claims 1-2, and 4-40 remain pending.

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. **Claims 1-2, and 4-19**, are rejected under 35 U.S.C. 103(a) as being unpatentable over Cheng et al (hereinafter "Cheng") U.S. Patent No. 2006/0282834 A1 in view of Sadwosky U.S. Patent No. 6,123,737.

5. As per **claim 1**, Cheng discloses a method of updating, the method comprising:

Informing a notification history server of notifications sent by authorized senders, the notification history server keeping a record of authorized notifications, the notifications history server being distinct from the authorized senders (***see fig. 1, which discloses service provider computer system 102 and software vendor computer system 103; 0109, which discloses alternatively software vendors who contract with the service provider may provide the information about their software products and software updates …directly to the service provider or to update database 709***);

receiving a notification in an electronic device that an update is available from a sender (***0109; 0115, which discloses that when a new software update or software product is available, the service provider computer 102 sends an email to those users who have requested notification by email…***); and

determining the authenticity of the received notification in the electronic device, by sending, by the electronic device, information retrieved from the received notification to the notification history server, and determining whether the notification history server has a record of the notification using information sent by the electronic device;

downloading the available update from the sender if the notification history server confirms knowledge (***0115, which discloses that if the software***

updates are approved by the user, the client application 104 downloads the software update, verifies its integrity…)

6. What Cheng does not explicitly teach is:

determining the authenticity of the received notification in the electronic device, by sending, by the electronic device, information retrieved from the received notification to the notification history server, and determining whether the notification history server has a record of the notification using information sent by the electronic device;

7. Sadowsky discloses

determining the authenticity of the received notification in the electronic device, by sending, by the electronic device, information retrieved from the received notification to the notification history server, and determining whether the notification history server has a record of the notification using information sent by the electronic device (***see figs. 3, which discloses authentic and valid 64; see fig. 4, which discloses push notification? … package authentic?; col. 4, lines 40-50, which discloses that the authenticity of the e-mail notification package 12 is tested … if the package 12 is found to be non-authentic, processing is terminated***…)

Accordingly it would have been obvious to one of ordinary skill in the art at time of applicant's invention to modify the method of Cheng and incorporate the method comprising determining the authenticity of the received notification in the electronic device, by sending, by the electronic device, information retrieved from the received notification to the notification history server, and determining whether the notification

history server has a record of the notification using information sent by the electronic device in view of the teachings of Sadowsky in order to ensure that the notice message is from the authorized vendor.

8. As per **claim 2,** Cheng further discloses the method, further comprising:

simultaneously informing the notification history server that a notification has been sent to the electronic device (see fig. 1; 0115).

9. As per **claim 4**, Cheng further discloses the method, further comprising:

ignoring the notification in the electronic device upon determining that the notification is inauthentic (see fig. 12);

recording that an inauthentic notification has been received (see fig. 12); and

waiting to receive another notification in the electronic device (see fig. 12).

10. As per **claim 5**, Cheng further discloses the method, further comprising:

determining identification information of a server and update package associated with the notification upon determining that the notification received in the electronic device is authentic (0012; 0040; 0079; 0082, which discloses identifying the location of the relevant updates files).

11. As per **claim 6**, Cheng further discloses the method, further comprising:

retrieving the update package (0082, which discloses downloads the software update files); and

performing an update of at least one of firmware and software resident in the electronic device (0083, which discloses that the software update is then installed).

12. As per **claim 7**, Cheng further discloses the method, wherein the notification comprises one of a short message service (SMS) notification, an instant messaging (IM) notification, an email notification, a wireless application protocol (WAP) push message notification, and an enhanced messaging service (EMS) notification (0114).

13. As per **claim 9**, Cheng failed to explicitly disclose the method, wherein determining the authenticity of the notification in the electronic device further comprises determining whether the notification was sent from an authorized server.

Sadowsky discloses the method, wherein determining the authenticity of the notification in the electronic device further comprises determining whether the notification was sent from an authorized server (col. 4, lines 40-50)

Accordingly it would have been obvious to one of ordinary skill in the art at time of applicant's invention to modify the method of Cheng and incorporate method, wherein determining the authenticity of the notification in the electronic device further comprises determining whether the notification was sent from an authorized server in view of the teachings of Sadowsky in order to ensure that the notice message is from the authorized vendor.

14. As per **claim 10**, Cheng further discloses the method, wherein an authorized server comprises one of a management server and a customer care center (see fig. 1).

15. As per **claim 11**, Cheng further discloses the method, wherein the notification comprises location and identification information regarding a management server providing access to an update package and information regarding the update package (0034, 0043; 0082).

16. As per **claim 12**, Cheng further discloses the method, wherein location and identification information comprise at least one of a universal resource locator (URL), an internet protocol (IP) address, a dynamic security key, end-user data, program update information, download scheduling information, and notification protocol information (see fig. 12; 0043; 0082).

17. As per **claim 13**, Cheng further discloses the method, further comprising retrieving an update package from a default management server by accessing an address of the default management server when no server address information is included in the notification, the address of the default management server being provisioned in the electronic device during a bootstrap provisioning event (see fig. 1; 0043).

18. As per **claim 14**, Cheng failed to explicitly disclose the method, wherein retrieving the update package from the default management server is performed after authentication of the notification message.

Sadowsky discloses the method, wherein retrieving the update package from the default management server is performed after authentication of the notification message (col. 4, lines 40-50)

Accordingly it would have been obvious to one of ordinary skill in the art at time of applicant's invention to modify the method of Cheng and incorporate method, wherein wherein retrieving the update package from the default management server is performed after authentication of the notification message in view of the teachings of Sadowsky in order to ensure that the notice message is from the authorized vendor.

19. As per **claim 15**, Cheng further discloses the method, further comprising:

retrieving an update package via a download agent in the electronic device (see fig. 2; 0082); and

updating at least one of firmware and software in the electronic device via an update agent in the electronic device (see fig. 2; 0083).

20. As per **claim 16**, Cheng further discloses the method, further comprising preventing unauthorized updates of at least one of firmware and software in the electronic device (see fig. 12).

21. As per **claim 17**, Cheng failed to explicitly disclose the method, wherein preventing unauthorized updates further comprises:

when a notification sent to the electronic device is discernable by an end-user and the end-user is prompted to initiate an update process, and when the end-user initiates the update process, the electronic device is adapted to determine the authenticity of the notification, and abort the update process if the notification is determined to be inauthentic, and permit the update package to be downloaded, if the notification is determined to be authentic.

Sadowsky discloses the method, wherein preventing unauthorized updates further comprises:

when a notification sent to the electronic device is discernable by an end-user and the end-user is prompted to initiate an update process, and when the end-user initiates the update process, the electronic device is adapted to determine the authenticity of the notification, and abort the update process if the notification is determined to be inauthentic, and permit the update package to be downloaded, if the notification is determined to be authentic (col. 4, lines 40-50).

Accordingly it would have been obvious to one of ordinary skill in the art at time of applicant's invention to modify the method of Cheng and incorporate method, wherein preventing unauthorized updates further comprises: when a notification sent to the electronic device is discernable by an end-user and the end-user is prompted to initiate an update process, and when the end-user initiates the update process, the electronic device is adapted to determine the authenticity of the notification, and abort the update

process if the notification is determined to be inauthentic, and permit the update package to be downloaded, if the notification is determined to be authentic in view of the teachings of Sadowsky in order to ensure that the notification message is from the authorized vendor.

22. As per **claim 18**, Cheng further discloses the method, wherein preventing unauthorized updates further comprises:

receiving a dynamic key component from a management server in the electronic device (0092; 0117);

accessing a static key component from memory in the electronic device (0117); and

instructing a download agent to use the dynamic key component and the static key component to generate a security key, wherein the generated security key facilitates access to a downloadable update package in an update package repository if the electronic device is authorized access to the update package, otherwise the electronic device is denied access to the update package (0082; 0092).

23. As per **claim 19**, Cheng further discloses the method, further comprising:

provisioning an address of a management server in the electronic device during a bootstrap provisioning event by sending a notification, the notification comprising server address information, and wherein the electronic device is adapted to access and

employ the address of the management server provisioned in the electronic device after the bootstrap provisioning event (0034).

24. **Claim 8**, is rejected under 35 U.S.C. 103(a) as being unpatentable over Cheng et al (hereinafter "Cheng") U.S. Patent No. 2006/0282834 A1 in view of Sadwosky U.S. Patent No. 6,123,737 as applied to claim 1 above, and further in view of Serbinis et al(hereinafter "Serbinis") U.S. Patent No. 6,314,425 B1.

25. As per **claim 8**, both Cheng and Sadowsky failed to explicitly disclose the method, wherein the electronic device comprises one of a mobile cellular phone handset, a personal digital assistant, a pager, an MP3 player, and a digital camera.

Serbinis discloses the method, wherein the electronic device comprises one of a mobile cellular phone handset, a personal digital assistant, a pager, an MP3 player, and a digital camera (col. 5, lines 30-52).

Accordingly it would have been obvious to one of ordinary skill in the art at time of applicant's invention to modify the method of Sadwosky and incorporate the method wherein the electronic device comprises one of a mobile cellular phone handset, personal digital assistant, pager, MP3 player, and a digital camera in view of the teachings of Serbinis in order to identify the equipment employed.

26. **Claims 20-22 and 24-38**, are rejected under 35 U.S.C. 103(a) as being unpatentable over Sadwosky U.S. Patent No. 6,123,737 in view of Serbinis et al U.S. Patent No. 6,314,425 B1.

27. As per **claim 20**, Sadowsky discloses a mobile services network at least comprising:

at least one electronic device (see fig. 1; client computer);

a management server communicatively linked with the at least one electronic device via a communication link; and

a notification history server operatively connected to the management server, the notification history server comprising a record of authentic notifications sent to the at least one electronic device by authorized senders, the authorized senders being distinct from the notification history server ***(see fig. 1, which discloses servers 2(1)…server(2(n));***

wherein the electronic device is adapted to determine the authenticity of a notifications received from a sender by contacting the notification history server and determining whether the notification history server has a record, from one of the authorized senders, of the notification received by the electronic device (***see figs. 3, which discloses authentic and valid 64; see fig. 4, which discloses push notification? … package authentic?; col. 4, lines 40-50, which discloses that the authenticity of the e-mail***

notification package 12 is tested … if the package 12 is found to be non-authentic, processing is terminated…).

28. What Sadwosky does not explicitly disclose is:

a management server communicatively linked with the at least one electronic device via a communication link

29. Serbinis discloses:

a management server communicatively linked with the at least one electronic device via a communication link (***see fig. 1, which discloses server computer 20 (1…n) coupled to the DMS database 25 and store 30***).

Accordingly it would have been obvious to one of ordinary skill in the art at time of applicant's invention to modify the method of Sadwosky by incorporating a distinct management server different from the notification server in view of the teachings of Serbinis in order to ensure that the notification package is authentic.

30. As per **claim 21**, Sadowsky further discloses the network, wherein the electronic device at least comprises:

non-volatile memory (fig. 1, client computer);

a short message entity; random access memory; and security services (fig. 1).

31. As per **claim 22**, Sadowsky further discloses the network, wherein the non-volatile memory in the electronic device at least stores:

an update agent (fig. 1);

a firmware and real-time operating system (fig. 1; col. 3, lines 5-20);

an operating system layer (fig. 1; col. 3, lines 5-20);

a download agent or browser (fig. 1); and

an end-user related data and content (see abstract; software package 18).

32. As per **claim 23**, Sadwosky failed to explicitly disclose the network, wherein the electronic device comprises one of a mobile cellular phone handset, personal digital assistant, pager, MP3 player, and a digital camera.

Serbinis discloses the network, wherein the electronic device comprises one of a mobile cellular phone handset, personal digital assistant, pager, MP3 player, and a digital camera (col. 5, lines 30-52).

Accordingly it would have been obvious to one of ordinary skill in the art at time of applicant's invention to modify the method of Sadwosky and incorporate the network comprising network, wherein the electronic device comprises one of a mobile cellular phone handset, personal digital assistant, pager, MP3 player, and a digital camera in view of the teachings of Serbinis in order to identify the equipment employed.

33. As per **claim 24**, Sadowsky failed to explicitly disclose the network, wherein the electronic device is adapted to receive notifications informing the electronic device of availability of update packages at the management server

Serbinis discloses the network, wherein the electronic device is adapted to receive notifications informing the electronic device of availability of update packages at the management server (col. 10, lines 50-60)

Accordingly it would have been obvious to one of ordinary skill in the art at time of applicant's invention to modify the method of Sadwosky by incorporating the network, wherein the electronic device is adapted to receive notifications informing the electronic device of availability of update packages at the management server in view of the teachings of Serbinis in order to ensure efficiency

34. As per **claim 25,** Sadwosky further discloses the network wherein the notification history server is adapted to determine whether a notification is authentic by examining message identification information in the notifications (see fig. 3 and 4; col. 4, lines 40-50).

35. As per **claim 26**, Sadwosky further discloses the network, wherein the electronic device is adapted to download an update package from an update package repository using an update agent upon determining that a notification received in the electronic device is authentic (see figs. 3 and 4; col. 4, lines 45-50).

36. As per **claim 27**, Sadwosky further discloses the network, wherein the electronic device is adapted to determine whether a notification originated from an authorized sender (col. 4, lines 45-50).

37. As per **claim 28**, Sadwosky further discloses the network, wherein an authorized sender is at least one of the management server and a customer care center resident in the network (fig. 3).

38. As per **claim 29,** Sadwosky failed to explicitly discloses the network, further comprising a short message center (SMC) adapted to store and forward messages to and from the electronic device, wherein the short message center (SMC) is adapted to send, upon instruction from the management server or a customer care center, notifications to the electronic device regarding availability of update packages.

Serbinis discloses the network, further comprising a short message center (SMC) adapted to store and forward messages to and from the electronic device, wherein the short message center (SMC) is adapted to send, upon instruction from the management server or a customer care center, notifications to the electronic device regarding availability of update packages (col. 10, lines 50-60)

Accordingly it would have been obvious to one of ordinary skill in the art at time of applicant's invention to modify the method of Sadwosky by incorporating the network, further comprising a short message center (SMC) adapted to store and forward messages to and from the electronic device, wherein the short message center (SMC) is adapted to send, upon instruction from the management server or a customer care center, notifications to the electronic device regarding availability of update packages in

view of the teachings of Serbinis in order to ensure that the notification package is authentic.

39. As per **claim 30**, Sadwosky further discloses the network, wherein notifications comprise at least one of a short message service (SMS) notification, an instant messaging (IM) notification, an email notification, a wireless application protocol (WAP) push message notification, and an enhanced messaging service (EMS) notification (see figs. 3, 4 and 5).

40. As per **claim 31**, Sadwosky further discloses the network, wherein notifications further comprise at least one user data field containing message identification information (fig. 5; col. 5, lines 50-65).

41. As per **claim 32**, Sadwosky failed to explicitly disclose the network, wherein notifications further comprise location and identification information regarding a management server providing access to an update package and information regarding the update package.

Serbinis discloses the network, wherein notifications further comprise location and identification information regarding a management server providing access to an update package and information regarding the update package (see fig. 1; col. 10, lines 50-60).

Accordingly it would have been obvious to one of ordinary skill in the art at time of applicant's invention to modify the method of Sadwosky by incorporating the network, wherein notifications further comprise location and identification information regarding a management server providing access to an update package and information regarding the update package in view of the teachings of Serbinis in order to ensure efficiency of the system.

42. As per **claim 33**, Sadwosky further discloses the network, wherein location and identification information comprise at least one of a universal resource locator, an internet protocol address, a dynamic security key, end-user data, program update information, download scheduling information, and notification protocol information (col. 6, line 30-35).

43. As per **claim 34**, Sadwosky further discloses the network, wherein upon determining that a notification received in the electronic device is inauthentic, the electronic device is adapted to ignore the notification and wait for another notification, and a record is created recording that an inauthentic notification has been received (col. 4, lines 40-50).

44. As per **claim 35**, Sadwosky further discloses the network, wherein the management server comprises the notification history server and an update package repository (fig. 1).

45. As per **claim 36**, Sadwosky further discloses the network, wherein the notification history server is incorporated into a short message center in the network (see fig. 1).

46. As per **claim 37**, Sadwosky further discloses the network, further comprising a security service in the electronic device for preventing unauthorized updating of at least one of firmware and software in the electronic device (col. 4, lines 40-50).

47. As per **claim 38**, Sadwosky further discloses the network, wherein preventing unauthorized updates further comprises:

when a notification sent to the electronic device is discernable by an end-user and the end-user is prompted to initiate an update process (col. 5, line 50-65), and

when the end-user initiates the update process, the electronic device is adapted to determine the authenticity of the notification, and abort the update process if the notification is determined to be inauthentic, and permit the update package to be downloaded, if the notification is determined to be authentic (col. 4, lines 40-65).

48. As per **claim 39**, Sadwosky failed to explicitly disclose the network, wherein preventing unauthorized updates further comprises:

receiving a dynamic key component from a management server in the electronic device;

accessing a static key component from memory in the electronic device; and

instructing a download agent to use the dynamic key component and the static key component to generate a security key, wherein the generated security key facilitates access to a downloadable update package in an update package repository if the electronic device is authorized access to the update package, otherwise the electronic device is denied access to the update package.

Serbinis discloses the network, wherein preventing unauthorized updates further comprises:

receiving a dynamic key component from a management server in the electronic device (col. 3, lines 40-50; col. 21, lines 30-50);

accessing a static key component from memory in the electronic device (col. 21, lines 30-50); and

instructing a download agent to use the dynamic key component and the static key component to generate a security key, wherein the generated security key facilitates access to a downloadable update package in an update package repository if the electronic device is authorized access to the update package, otherwise the electronic device is denied access to the update package (col. 21, lines 30-50).

Accordingly it would have been obvious to one of ordinary skill in the art at time of applicant's invention to modify the method of Sadwosky and incorporate the network comprising receiving a dynamic key component from a management server in the electronic device; accessing a static key component from memory in the electronic device; and instructing a download agent to use the dynamic key component and the

static key component to generate a security key, wherein the generated security key facilitates access to a downloadable update package in an update package repository if the electronic device is authorized access to the update package, otherwise the electronic device is denied access to the update package in view of the teachings of Serbinis in order to ensure adequate security.

49. As per **claim 40,** Sadwosky failed to explicitly disclose the network, wherein the network is adapted to provision the address of the management server in the electronic device during a bootstrap provisioning event by sending a notification, the notification comprising server address information, and wherein the electronic device is adapted to access and employ the address of the management server provisioned in the electronic device after the bootstrap provisioning event.

Serbinis discloses a the network, wherein the network is adapted to provision the address of the management server in the electronic device during a bootstrap provisioning event by sending a notification, the notification comprising server address information, and wherein the electronic device is adapted to access and employ the address of the management server provisioned in the electronic device after the bootstrap provisioning event (col. 21, lines 1-25)

Accordingly it would have been obvious to one of ordinary skill in the art at time of applicant's invention to modify the method of Sadwosky and incorporate the network comprising network, wherein the network is adapted to provision the address of the management server in the electronic device during a bootstrap provisioning event by

sending a notification, the notification comprising server address information, and wherein the electronic device is adapted to access and employ the address of the management server provisioned in the electronic device after the bootstrap provisioning event in view of the teachings of Hayes in order to ensure security.

Conclusion

50. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Charles C. Agwumezie whose number is **(571) 272-6838**. The examiner can normally be reached on Monday – Friday 8:00 am – 5:00 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Calvin Hewitt can be reached on **(571) 272 – 6709**.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Charlie C Agwumezie/
Primary Examiner, Art Unit 3685
December 16, 2009